



## Malware Prevention-TIPS &GUIDELINES TO FOLLOW:

### Malware:

- It is short for "malicious software."
- Software designed to infiltrate or damage a computer system without the users consent.

### Computer Virus:

- A computer virus is software that is malicious in nature and can copy itself.
- Usually infects a computer without the knowledge of the user.
- A computer virus is not spam, adware, or spyware, since they do not have the ability to reproduce.

### Spam:

- Usually a serious or criminal abuse email to send unsolicited bulk messages.
- It can apply also to Instant messaging, newsgroups, blogs, web search engines, and even mobile phones.
- Difficult or near impossible to hold the spammer accountable since the sender maybe in another country and/or spoofing a legitimate email address.

### "Rogue" anti-spyware applications also known as "scareware,":

- It is considered the most damaging malware since it involves simple user interactions, like clicking a web link, and can bypass virus protection.
- It generates erroneous or misleading alerts, or attempts to lure users into fraudulent transactions and may appear to be beneficial but provides limited or no security.
- Rogue security software might report a virus, even though your computer is actually clean.
- The software might also fail to report viruses when your computer is infected.
- Sometimes it will even install a virus or other malicious software on your computer so that the software has something to detect.
- A variety of malware software programs that prey on unsuspecting users by misleading them to believe they are actually installing a legitimate, helpful spyware-detection and removal tool.
- It will often mimic well-known brands such as Grisoft AVG, Norton and McAfee.



### **Social Networking Sites:**

- These sites focus on building online communities of people who share interests and/or activities.
- Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.
- MySpace, Facebook, and You Tube are the most widely use sites.
- Due to the enormous number of people using these sites, it is virtually impossible for them to police and secure against malware.

### **SYMPTOMS OF COMPUTER MALWARE INFECTION (TOP 10 Warnings):**

1. Continuous pop-ups, alerts or warnings that might say  
"Your computer is infected with a virus," even when not online or advising you to "Buy software RIGHT NOW!"
2. Your computer may dramatically slow down or be unable to browse the Internet.
3. You may experience ongoing computer lockups, or be unable to do a normal shutdown or restart.
4. Your legitimate applications may not open, especially Internet Explorer.
5. Producing false positives after a scan, either by branding a legitimate application as "spyware" or by discovering "spyware" that doesn't actually exist on the computer.
6. Once downloaded, the rogue software may refuse to uninstall by conventional means.
7. The antivirus software attempts to extort money by promising to fix or reverse the problem for a fee.
8. Rogue anti-virus/spyware programs often generate more "alerts" than the software made by reputable companies.
9. Other signs of infection include new desktop icons; new wallpaper, or having your default homepage redirected to another site.



## **PREVENTION STEPS:**

1. Never open an email attachment unless you are **POSITIVE** about the source.
2. Do **NOT** click on any pop-up that advertises anti-virus or anti-spyware software especially a program promising to provide every feature known to mankind.
3. The fakes often mimic well-known brands such as Grisoft AVG, Norton and McAfee.
4. Do **NOT** download freeware or shareware unless you have permission, since these programs often come bundled with spyware, adware or fake anti-virus programs. Free screensavers, for example, are notorious for having hidden payload.
5. Avoid questionable websites. Some sites may automatically download malicious software onto your computer.

**WHAT TO DO IF INFECTED:** If a strange virus alert message appears on your screen do the following:

1. Do **NOT** touch it or clicks anywhere near the alert message or icon.
2. Do **NOT** use your mouse to eliminate or scan for viruses
3. Do **NOT** use your mouse to close the message or alert window.
4. Do **NOT** continue to use the computer as you would normally.
5. Do **NOT** run your computer's antivirus software
6. **DO** immediately contact the a computer expert to help with removing the malware.